

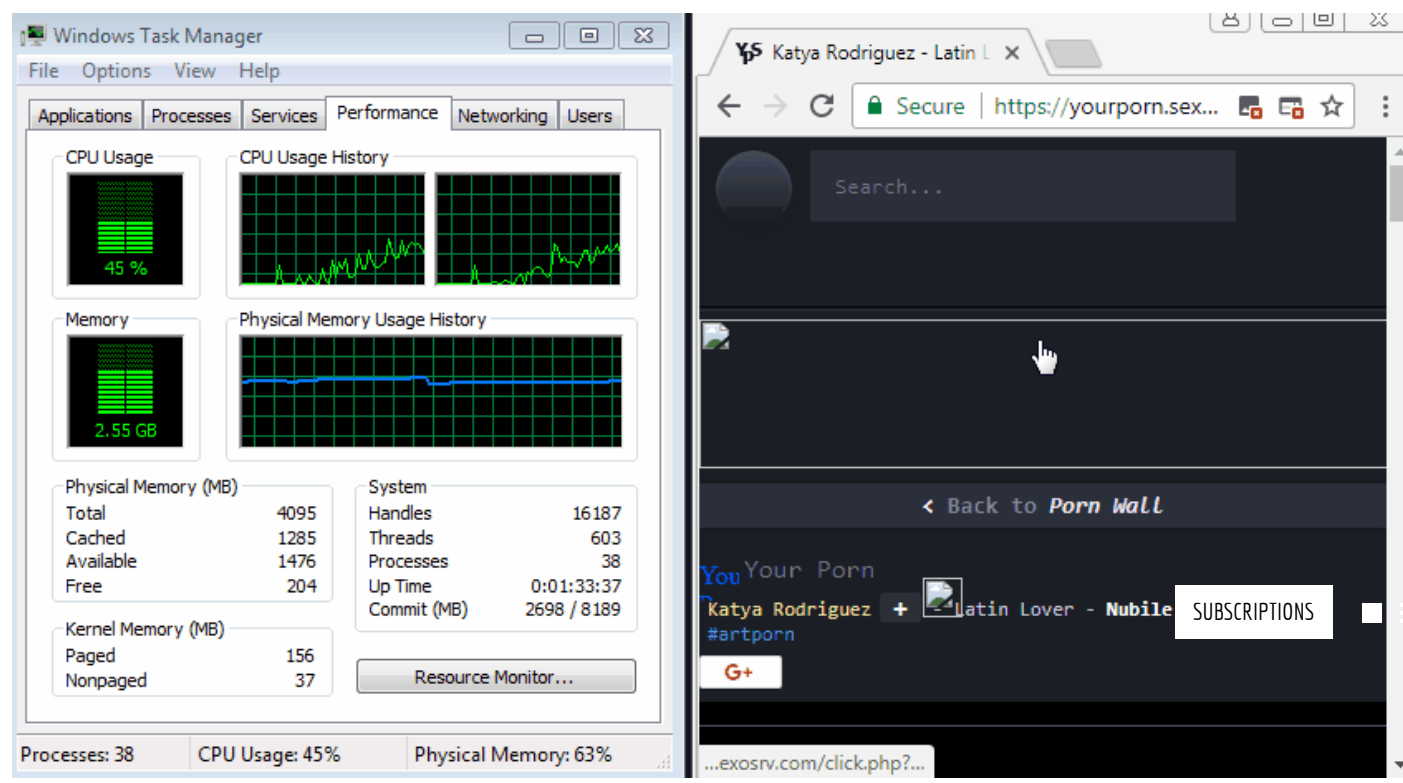


DON'T MINE ME, BRO —

Websites use your CPU to mine cryptocurrency even when you close your browser

Resource-draining code hides in pop-under windows that can remain open indefinitely.

DAN GOODIN - 11/30/2017, 5:10 AM



Researchers have discovered a new technique that lets hackers and unscrupulous websites perform in-browser, drive-by cryptomining even after a user has closed the window for the offending site.

Over the past month or two, drive-by cryptomining has emerged as a way to generate the cryptocurrency known as Monero. Hackers harness the electricity and CPU resources of millions of unsuspecting people as they visit hacked or deceitful websites. One researcher recently documented [2,500 sites actively running cryptomining code in visitors' browsers](#), a figure that, over time, could generate significant revenue. Until now, however, the covert mining has come with a major disadvantage for the attacker or website operator: the mining stops as soon as the visitor leaves the page or closes the page window.

Now, researchers from anti-malware provider Malwarebytes have identified a technique that allows the leaching to continue even after a user has closed the browser window. It works by opening a [pop-under window](#) that fits behind the Microsoft Windows taskbar and hides behind the clock. The

The animated GIF image at the top of this post shows the Windows task bar on the left. On the right is the offending browser window as the user removes it from its hiding place, resizes it, and finally closes it. In a [blog post published Wednesday morning](#), Malwarebytes Lead Malware Intelligence Analyst Jérôme Segura wrote:

This type of pop-under is designed to bypass adblockers and is a lot harder to identify because of how cleverly it hides itself. Closing the browser using the “X” is no longer sufficient. The more technical users will want to [run Task Manager](#) to ensure there is no remnant running browser processes and terminate them. Alternatively, the taskbar will still show the browser’s icon with slight highlighting, indicating that it is still running.

The Ad Maven ad network opens the pop-up window and loads a page hosted on elthamely[.]com. The page, in turn, loads resources from the Amazon content delivery network cloudfront.net. The Amazon resources retrieve a payload from yet another domain, hatevery[.]info.

Another way the new technique tries to conceal itself: the code running in the hidden browser window takes special care not to max out the CPU resources of the computer it’s running on. By throttling down the computationally intensive mathematical operations, the persistent mining stands a better chance of not being detected by end users.

Segura said the technique worked on the latest version of Chrome running on the latest versions of Windows 7 and Windows 10. At the moment, there are no indications the hidden window trick is being used against users of other browsers and operating systems, but don’t be surprised if that happens soon.

Listing image by [Lisa Brewster / Flickr](#)

Promoted Comments

digital0verdose / Smack-Fu Master, in training

[JUMP TO POST](#)

zneak wrote:

It's been a while since I've used Windows and I don't know how UX changes have made this harder to detect, but I'd like to see an entire screenshot of it. Back in my days, you'd still have a pretty obvious task bar icon for the outstanding window.

Most people who are above average when it comes to using a PC are likely not to be fooled by this... or not fooled for very long. However, there is a huge swath of users that are less savvy that this is going to impact. I'm sure there are plenty of people who will say that you shouldn't be using something you don't fully understand, but with the ubiquity in which computers are used in our day-to-day lives, that is not a realistic request. It would be like expecting everyone who drives a car to know how to fix it from end to end... or for those who talk about statistics to understand simple scientific principles.

25 posts | registered 5/18/2017

evan_s / Ars Tribunus Militum

[JUMP TO POST](#)

Bongle wrote:

zneak wrote:

It's been a while since I've used Windows and I don't know how UX changes have made this harder to detect, but I'd like to see an entire screenshot of it. Back in my days, you'd still have a pretty obvious task bar icon for the outstanding window.

By default, Windows has grouped icons nowadays (similar to the thing at the bottom on Mac). So you'd see the chrome icon, but it other than the slight shading, there'd be no `_strong_` indication that there's a window open.

If you turn off icon grouping in the taskbar (as you should...), then it returns to the "classic" XP-style, where every separate window has a separate item on the taskbar, which might make this more obvious.

Windows grouping, showing that IE is open: [http://in5stepstutorials.com/windows-7/ ... step-1.png](http://in5stepstutorials.com/windows-7/...step-1.png)

Disabled icon grouping: [http://in5stepstutorials.com/windows-7/ ... step-5.png](http://in5stepstutorials.com/windows-7/...step-5.png)

That's if the app is pinned to the start bar. If it isn't pinned then it disappears when the app is still open is pretty obvious but I do think having your

1867 posts | registered 5/20/2009

rabish12 / Ars Tribunus Angusticlavius

JUMP TO POST

evan_s wrote:

show nested quotes

That's if the app is pinned to the start bar. If it isn't pinned then it disappears when the app closes and the fact that a window is still open is pretty obvious but I do think having your main browser pinned is pretty common even among novice users.

Besides which the grouping means that there's no visible indication that the exploit is running if you have another browser window open on purpose. A lot of people never close their browsers, so this could run for a long time before they ever caught it.

9434 posts | registered 11/25/2009

DAN GOODIN

Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL dan.goodin@arstechnica.com // TWITTER [@dangoodin001](https://twitter.com/dangoodin001)

READER COMMENTS 169

SHARE THIS STORY

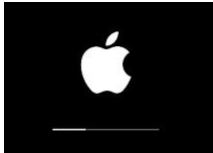
← PREVIOUS STORY

NEXT STORY →

Related Stories

Sponsored Stories

Powered by



Top 10 Antivirus (2018) - Who's Rated #1 For Mac?
www.antivirustop10.com



Take A Peek At This Insane Super Yacht
Mansion Global



Nippon Steel piggybacks on ArcelorMittal's bid for India's Essar
Nikkei Asian Review



Top 10 Mac Antivirus (2018) - Who's Rated #1 For Mac Users?
My Antivirus Review



Steph or KD? A fun question is about to get answers
espn.com/nba



Mandaluyong City Top 3 Discount Tire Deals for Sunday
Discount Tires Guide

Today on Ars

RSS FEEDS
VIEW MOBILE SITE
ABOUT US
SUBSCRIBE

CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS

NEWSLETTER SIGNUP

Join the Ars Orbital Transmission mailing list to get weekly updates delivered to your inbox.

Email address

SUBSCRIBE

WIRED Media Group

Use of this Site constitutes acceptance of our User Agreement (effective 1/2/14) and Privacy Policy (effective 1/2/14), and Ars Technica Addendum (effective 5/17/2012). View our Affiliate Link Policy. Your California Privacy Rights. The material on this site may not be reproduced, distributed, transmitted, cached or otherwise used, except with the prior written permission of Condé Nast.